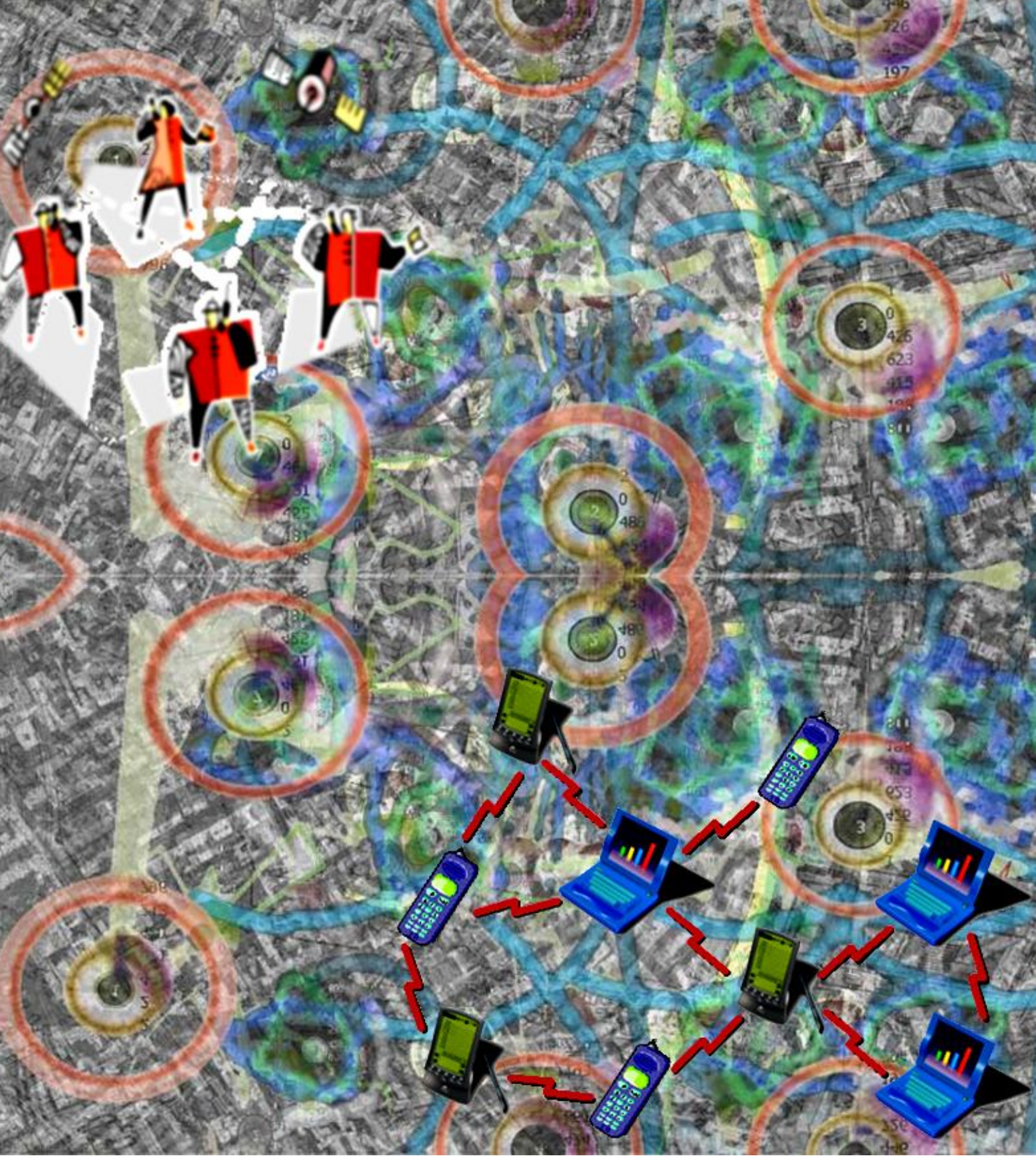

Paris Attack in Wireless Ad Hoc Network

Mohit Jain, Vishnu K

International Research Journal
ISSN 1839-6518
Vol. 1, No. 1, 2011
82800101201102

Paris Attack in Wireless Ad Hoc Network

Mohit Jain
Maharaja Surajmal Institute of Technology
New Delhi, India

Vishnu K.
Maharaja Surajmal Institute of Technology
New Delhi, India

International Research Journal
ISSN 1839-6518
Vol. 1, No. 1, 2011
82800101201102

Paris Attack in Wireless Ad Hoc Network

Abstract

Mobile Ad hoc networks are often used in places with little or no infrastructure. However its very nature of being dynamic and infrastructure less makes it vulnerable to many of the security related issues. In this paper we make use of the vulnerability present in the AODV protocol to present a new kind of Man in the Middle attack for MANETs namely, "The Paris Attack".

Keywords: Mobile Ad hoc Networks; Black Hole; Routing; AODV; Routing Table.

Introduction

A mobile Ad hoc network (MANET) is a network formed by a collection of nodes that are free to move around (mobile), leave and join the network at their wish. This kind of a network is beneficiary at places where building up an infrastructure is not feasible. Due to this lack of proper infrastructure and dynamic nature of MANETs it is prone to many security issues.

AODV [2] is one of the main routing protocols that are currently being used. Since AODV is a reactive protocol, whenever a node is ready to make a data transmission (say source node S) to any other node (say Destination node D) it starts the route discovery process. This is done by broadcasting a Route Request Packet (RREQ) to all of its neighbors. These packets are further transmitted to its neighbors and so on, until a node is found which has a fresh enough route to the Destination node (D) or the Destination node itself. In the either case the node replies back with a Route Response (RREP) to the node from which it received the RREQ. This RREP is further transmitted in the reverse direction till it reaches the Source node (S). The intermediate nodes update their routing tables whenever they receive an RREQ or an RREP packet with the next hop information.

Once the RREP packet reaches the Source node (S) it starts routing the data packets to the node from which it first received the RREP. This is because it is usually the shortest path. The packet is further passed on according to the next hop information of the intermediate nodes till it reaches the Destination node. Some researchers [3-11] discuss the vulnerabilities in Ad hoc routing protocols and the attacks that can be launched. The AODV protocol is vulnerable to many of the attacks. Some of them are The Black Hole

attack [3], Gray Hole Attack [6, 7], Rushing Attack [11], Worm Hole Attack [8-10] etc. A Black hole is a node that always answers positively for a Route Request (RREQ) even though it does not necessarily have a route. However once the data packets are routed through this node, it silently drops all the packets. A Black hole usually has a high probability of being chosen as a route because of two reasons: It doesn't have to check its routing table each time a RREQ is made to it. This reduces the computation time for the RREQ packet. It answers positively for every route request. On the other hand a Gray Hole is a node which behaves as normal node till a certain point of time but turns malicious later on. Also a Gray hole does not necessarily drop all the data packets, as in the case of a Black Hole. It may be selective towards specific nodes or specific kind of packets. Hence it is much more difficult to detect a Gray Hole in comparison to a Black Hole.

In this paper we present a new kind of attack for an ad hoc network that has the chances of being chosen as a valid route as high as that of a Black Hole & the stealth in the network much more than that of a Gray hole. The primary motive of the paper is to present a mechanism to intercept all the local network traffic around the malicious node without being detected. The rest of the paper is organized as follows. In section 2, we survey the related work. In section 3 the network model is given. In section 4, the proposed Methodology for the Attack is given. Finally in Section 5 we conclude and discuss future work.

Related Work

Recent researches have proposed many edible solutions to the above mentioned attacks. Many other attacks have also been proposed such as the Worm Hole Attack, the Rushing Attack, etc. Some of them have been briefed up below.

As explained earlier Juan [3] proposed the black hole injection attack in AODV according to which the malicious node replies positively for every RREP and hence gets into the route. It then silently drops all the data packets to be forwarded .Deng [4] has proposed an algorithm to prevent black hole attacks in ad hoc networks. Further S. Ramaswamy [5] proposed a solution to counter even the co-operative black hole attack. Since then many other solutions [4-7] have also been proposed. In case of a gray hole attack [6], it is a variation of the black hole, in which the nodes are initially not malicious but turns malicious later on. Also in such an attack the gray node may selectively drop data packets which make it further difficult to detect it. In order to counter this attack S.Banerjee [6] proposed that the total data traffic be divided into small sized blocks and

then perform an end to end checking. Many others [6-7] have also proposed various solutions.

In case of a wormhole attack [10], a node selectively transfers the packets that have routing information from one side of the network onto the other side by using a link. This shields the nodes near by the attackers from using any other alternative routes that has more than one or two hops. Hence making sure all the packets are routed through this link. Once, this tunnel is chosen for data transmission the attackers can drop/modify the data packets, selectively. A few solutions [8-10] have been proposed to counter wormholes as well.

And then there is the rushing attack [11] where an intermediate node rushes the forwarding of RREQ without updating its own routing table. This way it increases its chance of being chosen as a possible route. Once the communication link is established through this malicious node, it may behave similar to a worm hole by dropping/modifying data packets. In order to defeat the rushing attack many solutions have been proposed. One such solution proposed by Hu [11] randomizes and delays the forwarding of RREQ packets so that an RREQ rushing attacker cannot dominate other members during the RREQ phase.

Further there is the Check Sum Tamper attack [14] and the Port Change attack [13] where an intermediate node alters specific fields of the data packets that are being routed through it in a way that makes this data corruption stealthy and difficult to detect. The data corruption gives an overall effect of the data packets being dropped, however physically there is no packet dropping.

Network Model

We assume that the network nodes are randomly deployed across the network. We also assume that **c**ommunication is based on an on-demand routing protocol such as AODV.

Methodology

Our proposed attack mechanism is a variation of the Black Hole Attack. The major difference being that, in a Black Hole attack, the malicious node necessarily drops all the data packets that are being routed through it and does not have any valid route to the destination. But in our proposal the intention of the attack is to make the malicious node an intermediate node. This attack can be used to further pile up other attacks in MANETs such as the Port Change Attack [13] or the Check Sum Tamper Attack [14].

The attack approach proposed in this paper structures in three successive stages “Figure 1”:

- **STEP1:** When the source node S wants to route the data packets to the destination D, it floods the network with RREQ packets “Figure 2”. This is a common step in the functioning of any reactive protocol (such as AODV) as explained in Section 1. Whenever the node needs to route a packet it finds the route to its destination by flooding the RREQ and expects a RREP soon. The first node to reply with a RREP is chosen as the shortest route and the data is routed through it.
- **STEP2:** The malicious node (P) answers positively for every RREQ message it encounters with a RREP “Figure 3”. Note that the malicious node (P) doesn't have to look into its Routing table to reply with a RREP packet which saves the RREQ processing time. This move is the same as that of a Black Hole Attack. However the difference is observed because of Step 3.
- **STEP3:** The malicious node simultaneously finds a valid route itself to each of the victim node's destination (this is where the attack differs), by itself broadcasting a RREQ packet in search of a route to the destination node “Fig3”, “Fig4”.This RREQ is flooded to all other neighboring nodes except the one from which it received the earlier RREQ. This way the attacker has a valid route of each of the nodes it acts as an Intermediate Node “Figure 5”.

Since in Step 2 the attacking node (P), doesn't have to check its routing table, it is usually the first to respond to the RREQ in most cases and gets chosen as one of the routing nodes. Hence the motive of this attack, which is to intercept all of the local network traffic, is fulfilled.

The advantage of the extra link established is that the malicious node doesn't necessarily have to drop the intercepted data packets. Instead the node can corrupt the data packets by altering the data. This node would then be like the gateway to all the other local nodes. Hence Paris Attack can act as a precursor or a 1st stage to inject a malicious data intercepting node of any other Man in the Middle (MITM) attack [13, 14] above it. Another option is for the node to choose to be a silent Sniffer as in the case of a hacker which also may prove fatal to the Network Security.

It must be mentioned here that P can carry out other different types of attack by simply changing the way it manipulates the intercepted packets. The extra link also makes the detection mechanism more difficult. This will be more evident after the discussion below on detection strategies of other attacks.

Now here is why this attack proposal stands distinct. None of the detection methods used to detect a Black Hole, Gray Hole or a Worm Hole can be used to detect the Paris Attack.

In a traditional Black Hole attack the data packets are plainly dropped and hence the detection is easier. Let's look into some of the Black Hole detection methods and see why they don't apply here.

Deng et al [4] initially proposed an algorithm to prevent Black Holes. According to their algorithm any node receiving a RREP from an intermediate node crosschecks with the next hop on the route if it has a link to the node that sent the RREP and if it also has a link to the Destination node. Now in case of a Black Hole it gets caught as there isn't any valid route but in our proposed attack since a valid route and the link does exist, this detection algorithm would fail.

Later on S. Ramaswamy [5] extended the above detection method by intensive cross checking to solve co-operative Black Holes too. But since the basic idea of cross checking is the same, even this detection method would fail.

Then S. Banerjee [6] proposed an algorithm for detection of Black/Gray holes. The main idea being the flow of traffic was monitored by the neighbors of each node. However as we see in our attack as long as there is no explicit packet dropping the traffic flow is maintained and the attack can't be detected.

Further Marti [1] proposed the watchdog/pathrater algorithm in which every node has a watchdog which listens to the node's packet forwarding promiscuously. In case any of the nodes starts dropping the packet above a threshold, the watchdog accuses it to be malicious. Once again in this algorithm the watchdog can detect the malicious node only if there is a packet drop.

Gonzalez [12] also uses a similar concept in which the principal idea is the conservation of flow, meaning all packets sent to a node and not destined to that node are expected to exit the node. This is not violated in the Paris Attack and hence safe from detection.

Hence as we see most of the algorithms designed to detect other malicious attacks wouldn't suffice in detecting this attack. This makes Paris Attack stealthier than any other know attacks.

Conclusion and Future Work

In this paper we have fully presented the methodology of a new kind of attack in an ad hoc network. As future work we hope to

- Develop simulations to analyze the performance of the above attack.
- Develop an efficient solution to the above proposed attack.

Figures and Tables

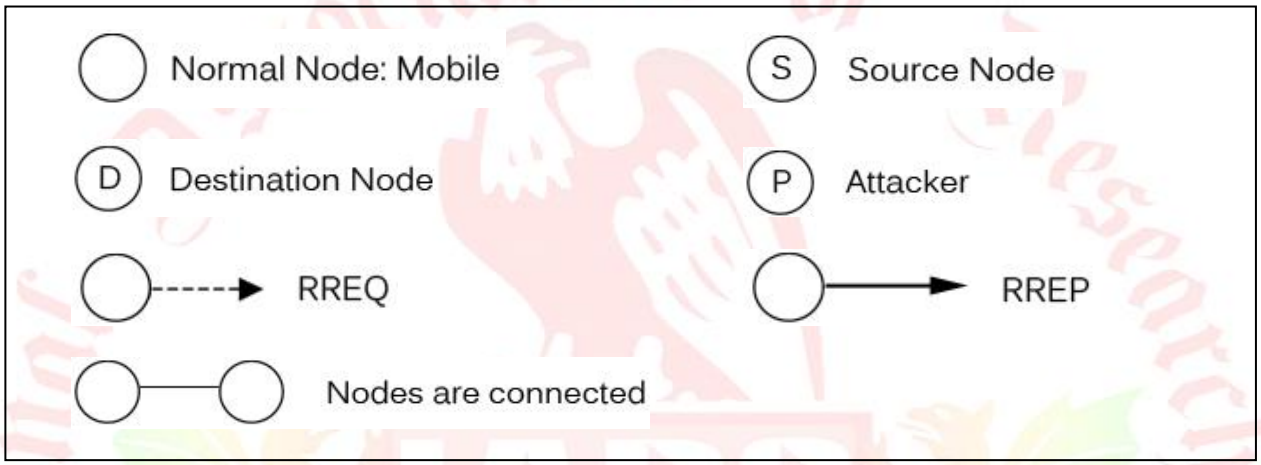

Figure 1: Representation of different nodes

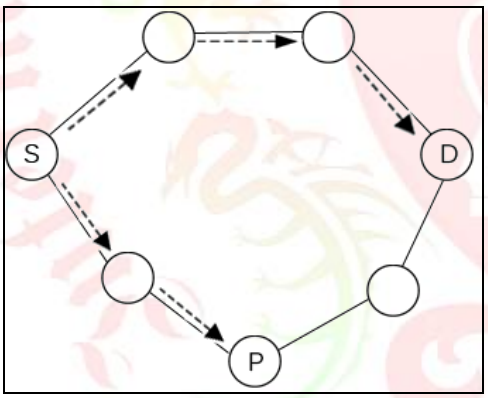

Figure 2: RREQ Flooding by Source Node.

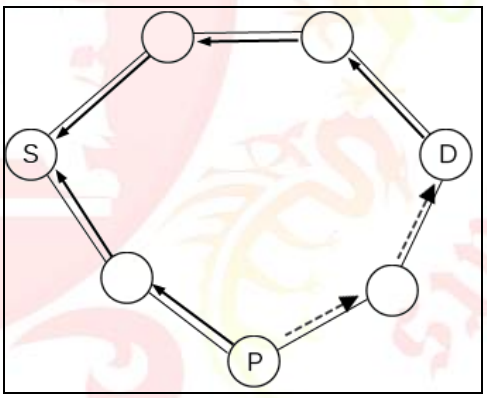

Figure 3: RREP by Attacker + RREQ in search of a valid route to D.

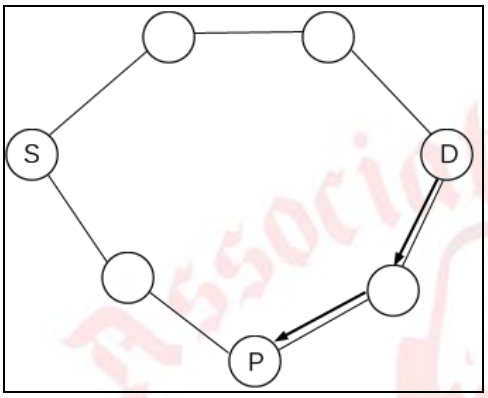

Figure 4: RREP by D to the Attacker P.

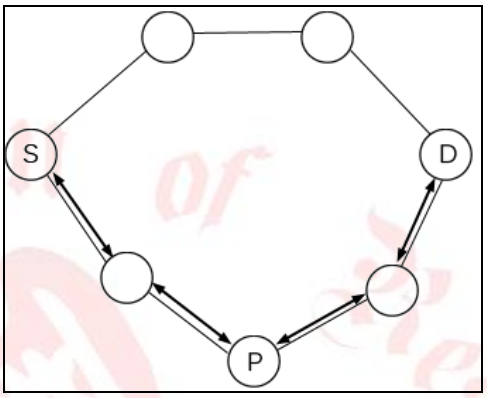

Figure 5: Final route from S to D

References

1. S.Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks". In Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 2000), August 2000.
2. Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, November 2002.
3. Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, "Black Hole Attack Injection in Ad hoc Networks", Instituto de las TIC Avanzadas (ITACA) Universidad Politécnica de Valencia, Campus de Vera s/n, E-46022, Valencia, Spain
4. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.
5. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.
6. Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA
7. Piyush Agrawal, R. K. Ghosh, Sajal K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks" In Proceedings of the 2nd international

conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

8. Ritesh Maheshwari, Jie Gao and Samir R Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information", Department of Computer Science, Stony Brook University Stony Brook.
9. L.Lazos, R. Poovendran, C. Meadows, P. Syverson , L.W.Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", University of Washington, Seattle, Washington, Naval Research Laboratory, Washington, DC
10. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", IEEE INFOCOM, 2003.
11. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", ACM WiSe'03 in conjunction with MOBICOM'03, pages 30– 40, 2003.
12. Oscar F. Gonzalez, Michael Howarth, and George Pavlou, "Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks", Center for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.
13. Vishnu K, Mohit Jain and Shalini Jain, "A new Attack proposal for wireless Ad hoc Networks", International Journal of Computer Science and Network Security (IJCSNS) Vol. 10 No. 8 pp. 146-148
14. Vishnu K, "A new kind of Transport Layer attack in Wireless Ad hoc Networks", Wireless Communications, Networking and Information Security (WCNIS), IEEE International Conference 2010

– END –

International Association of Research Scholars

IARS

Transforming Research

Since 2011

www.iars.info

Certificate of Recognition

This certificate is awarded to

Mohit Jain

in recognition of his / her contribution

"Paris Attack in Wireless Ad Hoc Network"

to Vol. 01, No. 01, 2011 *of*

IARS International Research Journal

An International Refereed Research Journal

ISSN 1839-6518 (Australian ISSN Agency)

Editor in Chief

IARS International Research Journal 08 FEB 2011